Community-based Coordinated Services System

Securing Client Confidentiality

The Community-based Coordinated Services System has been meticulously designed to ensure confidentiality of client records. Locked access prevents unauthorized use and need-to-know barriers ensure that a specific agency or service provider has access only to the information necessary to assist the client. All clients have the choice of whether or not to share their information and authorization by the client initiates inclusion into the system.

HIPAA Compliance

The Community-based Coordinated Services System provides secure, confidential and HIPAA-compliant tracking of each call, follow-up management and data collection. HIPAA compliance is ensured in the following ways:

1. The system only stores encrypted Social Security numbers.
2. Data are encrypted during data transfer and are not decoded until it is confirmed that the data has been received by the correct recipient machine.
3. Data are protected by a three-tier architecture.
4. After five errant password logins, a lockout function is activated.
5. A firewall physically limits access to the core data set.
6. SeniorNavigator has business associate agreements with all service providers, subcontractors and staff to maintain the privacy of participant data.

System Security

General System Security: Web-based services are provided through a secure service environment with redundant T-3 connections to ensure 24/7 system operation and availability. The server has co-location sites which provide a secure environment with restricted access through a sophisticated handprint identification system. Diesel back-up generators are provided for ongoing power. Back-up functions are part of the online system. Information is maintained in two parallel systems.

Disaster Protection: There are servers in secure locations on each coast and a tertiary hosting facility in Oakland, California. All data backups are stored in multiple locations. During production equipment upgrades, continuous system operations are ensured by switching between sites.

Role-Based Access Controls: The system accommodates several hundred permutations of user permissions for security purposes and enables system administrators to limit access of users at the module level. Each of the modules in the system allows users to assign the following access levels: administrative, full, read-only and none. User passwords are protected with a 64-bit encryption technology.

Platform Utilized:

The operating system of the server is Linux and the tools are created in JAVA. Enterprise systems also are created and maintained in FoxPro, such as HOMCare, MSSPCare, PACECare and CADCare.

The Community-based Coordinated Services System has been designed for flexibility and existing files can be transferred into it through a variety of formats, including Excel, SQL and Access.

User Security Agreements:

Every agency or organization in the Community-based Coordinated Services System must agree in writing that it will:

- Uphold federal and state confidentiality regulations and laws that protect client records and will not release confidential client records without written consent of the client, or the client's guardian, unless otherwise provided for in the regulations or laws.
- Abide specifically by federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records. In general, the federal regulation prohibits the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. (A general authorization for the release of medical or other information is not sufficient for this purpose.)
- Abide specifically with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and corresponding regulations passed by the U.S. Department of Health and Human Services. In general, the regulations provide clients with new rights to control the release of medical information, including advance consent for most disclosures of health information, the right to see a copy of health records, the right to request correction to health records, the right to obtain documentation of disclosures of their health information and the right to an explanation of their privacy rights and how information may be used or disclosed. The current regulation provides for protection for paper, oral and electronic information.

In addition, these organizations must:

- Limit access to authorized users and follow all protocols to monitor those users.
- Provide SeniorNavigator with the names of all staff members and volunteers who have access to the system and certify that such staff are competent and authorized to have access to this information.
- Agree that SeniorNavigator may deny access to the system for the purpose of investigating any suspicion of breached confidentiality.
- Notify SeniorNavigator prior to or immediately following changes relating to authorized users.

Through these safeguards, the Community-based Coordinated Services System has been engineered to be a most secure tool for both ensuring client confidentiality and improving the delivery of services to seniors and adults with disabilities.